98 227 #2

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 １月２１日

願 番 号
Application Number: 平成１１年特許願第０１３２１５号

願 人
Applicant (s): インターナショナル・ビジネス・マシーンズ・コーポレイション

CERTIFIED COPY OF PRIORITY DOCUMENT

１９９９年 ５月１４日

特 許 庁 長 官
Commissioner,
Patent Office 伊佐山建志

【書類名】　特許願

【整理番号】　JA998227

【あて先】　特許庁長官　殿

【国際特許分類】　G08B 13/00

G08B 13/24

G06F 1/00

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビ
ー・エム株式会社　大和事業所内

【氏名】　田　中　順

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビ
ー・エム株式会社　大和事業所内

【氏名】　堀　越　秀　人

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビ
ー・エム株式会社　大和事業所内

【氏名】　野　村　雅　彦

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビ
ー・エム株式会社　大和事業所内

【氏名】　臼　井　英　之

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビ
ー・エム株式会社　大和事業所内

【氏名】　堀　越　正　太

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビ
ー・エム株式会社　大和事業所内

【氏名】　田　村　　文　雄

【特許出願人】

【識別番号】　390009531

【住所又は居所】　アメリカ合衆国１０５０４、ニューヨーク州アーモンク（番地なし）

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレイション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【連絡先】　０４６２－７３－３３１８、３３２５、３４５５

【選任した代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【手数料の表示】

【予納台帳番号】　024154

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9304391

【包括委任状番号】　9304392

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セキュリティ機能付きコンピュータおよび方法

【特許請求の範囲】

【請求項１】コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、

（ａ）前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、

（ｂ）前記ステップ（ａ）のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、

（ｃ）前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出するステップと、

（ｄ）前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出するステップと、

（ｅ）前記ステップ（ｃ）およびステップ（ｄ）に応答して前記コンピュータへのアクセスを禁止するステップと

を有する方法。

【請求項２】前記ステップ（ｂ）を、前記コンピュータのパワー・オン、省エネ・モードの変更、および特定のファイルへのアクセスからなるグループから選択された一つの要素に応答して開始する請求項１記載の方法。

【請求項３】前記ステップ（ｅ）を適切なパスワードの入力がない場合にのみ実行する請求項１記載の方法。

【請求項４】コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、

（ａ）前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、

（ｂ）前記ステップ（ａ）のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、

（ｃ）前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出するステップと、

（ｄ）前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出するステップと、

（ｅ）前記ステップ（ｃ）およびステップ（ｄ）に応答して、装着されたことがある前記セキュリティ装置が現在脱着されていることを示すデータを前記第一の記憶手段の第二の記憶領域に記憶し保持するステップと、

（ｆ）前記ステップ（ｅ）に応答して前記コンピュータへのアクセスを禁止するステップと

を有する方法。

【請求項５】コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、

（ａ）前記コンピュータに装着されたセキュリティ装置が脱着されたことを示すデータを前記コンピュータに装備された第一の記憶手段の第二の記憶領域に記憶するステップと、

（ｂ）前記ステップ（ａ）のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、

（ｃ）前記第二の記憶領域のデータに基づいて前記装着されたセキュリティ装置が脱着されたことを検出するステップと、

（ｄ）前記ステップ（ｃ）に応答して前記コンピュータへのアクセスを禁止するステップと

を有する方法。

【請求項６】コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、

（ａ）前記コンピュータに前記セキュリティ装置が装着されたことを示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、

（ｂ）前記コンピュータから前記セキュリティ装置が脱着されていないか否かを前記コンピュータに装備された演算処理装置が定期的に監視するステップと、

（ｃ）前記ステップ（ｂ）に応答して前記コンピュータへのアクセスを禁止するステップと

を有する方法。

【請求項７】セキュリティ装置の装着ができるコンピュータであって、

前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶手段と、

演算処理装置と、

（ａ）前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、（ｂ）前記ステップ（ａ）のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、（ｃ）前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出するステップと、（ｄ）前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出するステップと、（ｅ）前記ステップ（ｃ）およびステップ（ｄ）に応答して前記コンピュータへのアクセスを禁止するステップとを前記コンピュータに実行させるプログラムとを記憶したコンピュータによる読みとりが可能な第二の記憶手段と

を有するコンピュータ。

【請求項８】セキュリティ装置の装着ができるコンピュータであって、

前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶手段と、

演算処理装置と、

（ａ）前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、（ｂ）前記ステップ（ａ）のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、（ｃ）前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出するステップと、（ｄ）前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出するステップと、（ｅ）前記ステップ（ｃ）およ

びステップ（ｄ）に応答して、装着されたことがある前記セキュリティ装置が現在脱着されていることを示すデータを前記第一の記憶手段の第二の記憶領域に記憶し保持するステップと、（ｆ）前記ステップ（ｅ）に応答して前記コンピュータへのアクセスを禁止するステップとを前記コンピュータに実行させるプログラムとを記憶したコンピュータによる読みとりが可能な第二の記憶手段と
を有するコンピュータ。

【請求項９】セキュリティ装置の装着ができるコンピュータであって、

前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶手段と、

演算処理装置と、

（ａ）前記コンピュータに装着されたセキュリティ装置が脱着されたことを示すデータを前記コンピュータに装備された第一の記憶手段の第二の記憶領域に記憶するステップと、（ｂ）前記ステップ（ａ）のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、（ｃ）前記第二の記憶領域のデータに基づいて前記装着されたセキュリティ装置が脱着されたことを検出するステップと、（ｄ）前記ステップ（ｃ）に応答して前記コンピュータへのアクセスを禁止するステップとを前記コンピュータに実行させるプログラムとを記憶したコンピュータによる読みとりが可能な第二の記憶手段と
を有するコンピュータ。

【請求項１０】セキュリティ装置の装着ができるコンピュータであって、

前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶手段と、

演算処理装置と、

（ａ）前記コンピュータに前記セキュリティ装置が装着されたことを示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、（ｂ）前記コンピュータから前記セキュリティ装置が脱着されたか否かを前記コンピュータに装備された演算処理装置が定期的に監視するステップと、（ｃ）前記ステップ（ｂ）に応答して前記コンピュータへのアクセスを禁止するステップとを前記コンピュータに実行させるプログラムとを記憶した

コンピュータによる読みとりが可能な第二の記憶手段と
を有するコンピュータ。

【請求項１１】セキュリティ装置の着脱ができるコンピュータであって、

前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶手段と、

演算処理装置と、

前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記第一の記憶手段の第一の記憶領域に記憶させる手段と、

前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出する手段と、

前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出する手段と、

前記検出手段に応答して前記コンピュータへのアクセスを禁止する手段と
を有するコンピュータ。

【請求項１２】セキュリティ装置の着脱ができるコンピュータであって、

前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶手段と、

演算処理装置と、

前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記第一の記憶手段の第一の記憶領域に記憶させる手段と、

前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出する第一の検出手段と、

前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出する第二の検出手段と、

前記第一および第二の検出手段に応答して、装着されたことがある前記セキュリティ装置が現在脱着されていることを示すデータを前記第一の記憶手段の第二の記憶領域に記憶させる手段と、

前記第二の記憶領域に記憶されたデータに応答して前記コンピュータへのアクセスを禁止する手段と

を有するコンピュータ。

【請求項１３】セキュリティ装置の装着ができるコンピュータであって、

前記コンピュータの主電源が停止している状態で記憶保持が可能な第一の記憶手段と、

演算処理装置と、

前記コンピュータに装着されたセキュリティ装置が脱着されたことを示すデータを前記第一の記憶手段の第二の記憶領域に記憶させる手段と、

前記第二の記憶領域のデータに基づいて前記装着されたセキュリティ装置が脱着されたことを検出する検出手段と、

前記検出手段に応答して前記コンピュータへのアクセスを禁止する手段と

を有するコンピュータ。

【請求項１４】セキュリティ装置の装着ができるコンピュータであって、

前記コンピュータの主電源が停止している状態で記憶保持が可能が第一の記憶手段と、

前記コンピュータに前記セキュリティ装置が装着されたことを示すデータを前記第一の記憶手段の第一の記憶領域に記憶させる手段と、

前記コンピュータから前記セキュリティ装置が脱着されたか否かを定期的に監視する演算処理装置と、

前記前記演算処理装置の監視結果に応答して前記コンピュータへのアクセスを禁止する手段と

を有するコンピュータ。

【請求項１５】前記第一の記憶手段がＲＦＩＤシステムに使用するＲＦＩＤタグであり、前記セキュリティ装置がＲＦアンテナである請求項７ないし請求項１４のいずれかに記載のコンピュータ。

【請求項１６】前記ＲＦアンテナが前記コンピュータのデバイス・ベイの蓋に装着されている請求項７ないし１４のいずれかに記載のコンピュータ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータの盗難および不正アクセス等を防止するためにコンピュータ本体に取り外し可能に装着されたセキュリティ機能の一部を担う装置が不正に取り外された場合に、コンピュータへのアクセスを禁止する技術に関する。

【０００２】

【従来の技術】

ノートブック型コンピュータは携帯性に優れている反面、きわめて容易に不正に外部に持ち出される。近年のコンピュータ利用の高度化および多様化に伴い、ユーザは貴重な情報をコンピュータ内部に格納する傾向がますます強まり、コンピュータが盗難に合うとその物理資源の損失に比べて情報資源の漏洩による損失が一層甚大になってきている。

【０００３】

特開平８－５０６９０号公報および特開平１０－１２４７６４号公報は、ＲＦ（ラジオ周波数）トランスポンダ・システムという非接触的な通信技術を用いた電子式物品監視システムを開示する。ＲＦトランスポンダ・システムは、一般的に励振器（Exicter）／読取器（Reader）すなわちＥＲ、およびＲＦＩＤトランスポンダあるいはＲＦＩＤ（Radio Frequency Identification）タグと呼ばれるものを含んでいる。監視区域内の物品にＲＦＩＤタグを取り付け、その領域の出入口にＥＲを設置して常時ＲＦ励振信号を発生させる。出入口にＲＦＩＤタグが取り付けられた物品が接近するとＥＲがこれに励振信号を送信して電力を与えるのでＲＦＩＤタグ自体は特に動作用の電力を必要としない。ＲＦ励振信号を受け取ったＲＦＩＤタグは識別コードその他のデータ信号を発生し、特定の周波数でＥＲに応答信号として送り返す。この応答信号中に含まれる識別コードをＥＲが検出すると必要に応じてアラーム音を発生して物品の盗難を防止する。物品を監視区域内からアラーム音を発生させないで持ち出すには、ＲＦＩＤタグをアラーム信号を送信しない状態にセットするかこれを脱着する必要がある。

【０００４】

特開平５－３５３５４号公報は、ノートブック型コンピュータの盗難防止を図る技術を開示する。ノートブック型コンピュータに、設置傾斜量、設置圧力および設置距離等の設置状態の変化を検出する盗難防止手段と設置状態の変化に応答

して警報を発する手段を設ける。これらの手段が機能を発揮する状態にあるときコンピュータは設置状態を常時監視し、コンピュータを許可なく定位置から持ち運ぼうとした際に警報を発して盗難を防止する。

【０００５】

特開平３－１００８９４号公報は、携帯端末が盗難に合ったときにキー入力を停止して不正なアクセスを禁止する技術を開示する。携帯端末が盗難に合うと、ホストコンピュータから無線で端末に特定の信号を送り、それに応答して端末内部のプログラムが作動してキー入力ができない状態にする。

【０００６】

【発明が解決しようとする課題】

上述したようにＲＦＩＤタグを使用して物品の盗難を防止する技術が知られており、またノートブック型コンピュータが監視区域から不正に持ち出されることを防止する技術およびコンピュータの盗難時にキー入力をロックして情報資源を保護する技術も知られている。しかし、ＲＦＩＤタグをコンピュータに装着して盗難に合ったコンピュータへの不正アクセスを防止する技術は開示されていない。

【０００７】

ところで、盗難防止または記憶情報への不正アクセスを防止するには、コンピュータにＲＦＩＤタグのような装置を装備する必要がある。一方このような装置は、すべてのユーザが必要とするものではなく、一般に企業内で大規模に使用している場合に比べて個人的範囲でのみ使用するユーザにとっては必要性が少ない。セキュリティ機能をすべてのコンピュータに装備して販売することは、必要のないユーザに対して余分な費用を強いることになり好ましくない。したがって、特定のシリーズに含まれる同一タイプのコンピュータにおいて、セキュリティ機能を装備するものとセキュリティ機能を装備しないものとを用意する必要がある。

【０００８】

ところで、特定のシリーズに含まれるコンピュータは、できるだけハードウエアおよびソフトウエアの共通化を図ることが販売コストおよび販売後のサービス

の維持という面で好ましい。特定のシリーズのコンピュータをセキュリティ機能を装備するものと装備しないものとに分けて製造および販売することは、一見セキュリティ機能を必要としないユーザの費用負担を公平にできるようにみえるが、共通化ができない部分での費用負担が増加し結果としてそのようなユーザにとっても不利になる。ここに、ハードウエアおよびソフトウエアの共通化とユーザによるセキュリティ機能の選択による費用負担の公平性という課題を同時に解決する必要が生じてくる。

【０００９】

これを解決する方法として、あるセキュリティ機能が複数のハードウエアおよびソフトウエアの構成要素からなる場合にその構成要素のある部分までを共通にし、残りの一部を販売店またはユーザが必要に応じて追加できるオプショナル部品にしてセキュリティ機能を完成できるようにする方法がある。しかし、セキュリティ機能の一部を担う装置をユーザまたは販売店で装着するようにすると（このような装置を以後単にセキュリティ装置という。）、その部分が不正に脱着されてセキュリティ機能が毀損されてしまうことが予測される。

【００１０】

したがって本発明の目的は、コンピュータのセキュリティ機能を担う一部の装置、すなわちセキュリティ装置がコンピュータから不正に脱着されたときに、コンピュータへのアクセスを禁止する技術を提供することにある。さらに本発明の目的は、セキュリティ機能を備えるコンピュータと備えないコンピュータとの間でセキュリティ装置のみをオプショナルとし、他のハードウエアおよびソフトウエアは両コンピューに共通のものを組み込んだコンピュータを提供することにある。さらにまた本発明の目的は、ユーザまたは販売店がオプショナルに取り付けるセキュリティ装置の好適な取り付け構造を提供することにある。

【００１１】

【課題を解決するための手段】

本発明に係るコンピュータはセキュリティ装置をオプショナルに取り付けることができる構造を備え、セキュリティ装置を装着することによりセキュリティ機能を具備したコンピュータを構成し、セキュリティ装置を脱着することでセキュ

リティ機能を具備しないコンピュータを構成する。本発明においてコンピュータへのアクセスを禁止する手順は、コンピュータのパワー・オン、省エネ・モードの変更、特定のファイルへのアクセス等の特定のイベントに関連付けて開始させることができるが、常時ＣＰＵにポーリングにより監視させてもよい。特定のイベントに関連付けて開始させると、ＣＰＵの負担を軽くすることができる。

【００１２】

本発明の一の態様では、コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、（ａ）前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、（ｂ）前記ステップ（ａ）のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、（ｃ）前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出するステップと、（ｄ）前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出するステップと、（ｅ）前記ステップ（ｃ）およびステップ（ｄ）に応答して前記コンピュータへのアクセスを禁止するステップとを備える。

【００１３】

本発明においてセキュリティ装置とは、コンピュータのセキュリティ機能の一部を担うハードウエアであって、オプショナル部品として用意されユーザまたは販売店で脱着可能な程度の装着容易性を備える装置をいう。たとえばＲＦＩＤを利用したセキュリティ・システムではＲＦアンテナでもよく、指紋検出を利用したセキュリティ・システムでは指紋入力部であってもよい。第一の記憶手段はコンピュータの主電源が停止した状態で記憶内容を保持できる記憶媒体でＥＥＰＲＯＭまたはハードディスク等を選定できる。さらに二次電池により主電源が停止している場合でも記憶保持ができる電力が供給され続けているＲＡＭであってもよい。この手順はセキュリティ機能を備えるコンピュータおよび備えないコンピュータのいずれに対しても共通に実行でき、セキュリティ機能を備えるコンピュータについてのみセキュリティ装置が脱着されたときにアクセスが禁止される。

【００１４】

上記第一の態様においては、ステップ（ａ）により、このコンピュータがセキュリティ機能を備えたコンピュータであることがシステムにより認識され、コンピュータからセキュリティ装置が脱着された場合は不正行為があったものとして以下の手順によりパスワードを入力しない限りコンピュータへのアクセスが禁止される。ステップ（ｂ）によりコンピュータへのアクセスを禁止する手順がセキュリティ機能を備えるコンピュータにもセキュリティ機能を備えないコンピュータにも開始される。ステップ（ｃ）により、このコンピュータがセキュリティ機能を備えるコンピュータであることが確認される。ステップ（ｄ）によりコンピュータからセキュリティ装置が脱着されていることが確認され、これは不正行為としてステップ（ｅ）でコンピュータへのアクセスが禁止される。適正にセキュリティ装置を脱着する場合は、パスワードを入れてアクセスを確保することができる。

【００１５】

本発明の第二の態様は、コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、（ａ）前記コンピュータに前記セキュリティ装置が装着されたこと示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、（ｂ）前記ステップ（ａ）のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、（ｃ）前記第一の記憶領域のデータに基づいて前記コンピュータに前記セキュリティ装置が装着されたことがあることを検出するステップと、（ｄ）前記コンピュータから現在前記セキュリティ装置が脱着されていることを検出するステップと、（ｅ）前記ステップ（ｃ）およびステップ（ｄ）に応答して、装着されたことがある前記セキュリティ装置が現在脱着されていることを示すデータを前記第一の記憶手段の第二の記憶領域に記憶し保持するステップと、（ｆ）前記ステップ（ｅ）に応答して前記コンピュータへのアクセスを禁止するステップとを備える。

【００１６】

上記態様のステップ（ｅ）では、一旦セキュリティ装置が装着されてこのコンピュータがセキュリティ機能を備えるコンピュータであることをシステムが認識

したのちにセキュリティ装置が取り外されたことがある場合は、そのコンピュータに対して不正なアクセスがあったことを示すデータとして記憶させる。このデータは、以後リセットされない限り第二の記憶領域に記憶保持される。

【００１７】

本発明の第三の態様では、コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、（ａ）前記コンピュータに装着されたセキュリティ装置が脱着されたことを示すデータを前記コンピュータに装備された第一の記憶手段の第二の記憶領域に記憶するステップと、（ｂ）前記ステップ（ａ）のあとに前記コンピュータへのアクセスを禁止する手順を開始するステップと、（ｃ）前記第二の記憶領域のデータに基づいて前記装着されたセキュリティ装置が脱着されたことを検出するステップと、（ｄ）前記ステップ（ｃ）に応答して前記コンピュータへのアクセスを禁止するステップとを備える。

【００１８】

ステップ（ａ）のデータは、本発明の第二の態様で示した方法で記憶してもよい。ステップ（ｃ）でこのデータを確認することにより、ステップ（ｂ）で開始した手順の実行段階ではセキュリティ装置が装着されていたとしても、それ以前に少なくとも一度はセキュリティ装置が脱着されたことがあるのでコンピュータへのアクセスが禁止される。

【００１９】

本発明の第四の態様では、コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、（ａ）前記コンピュータに前記セキュリティ装置が装着されたことを示すデータを前記コンピュータに装備された第一の記憶手段の第一の記憶領域に記憶し保持するステップと、（ｂ）前記コンピュータから前記セキュリティ装置が脱着されたか否かを前記コンピュータに装備された演算処理装置が定期的に監視するステップと、（ｃ）前記ステップ（ｂ）に応答して前記コンピュータへのアクセスを禁止するステップとを備える。

【００２０】

ステップ（ｂ）では、セキュリティ機能を備えるコンピュータにおいて演算処理装置にセキュリティ装置が脱着されたことを定期的に監視させる。この場合はコンピュータの電源が入っていることが前提になるが、セキュリティ装置が脱着されたあとに演算処理装置の定期的な監視のタイミングでアクセスを禁止することができる。

【００２１】

本発明の第一ないし第四の態様で説明した各ステップは、コンピュータ・プログラムによりコンピュータ上で実行させることができる。このようなプログラムは第二の記憶手段として利用できるＥＥＰＲＯＭまたはＦＬＡＳＨ　ＲＯＭといわれる不揮発性のメモリや、ハードディスク、フロッピー・ディスク等に記憶させることができ、コンピュータの動作時にメイン・メモリに読み出して演算処理装置で実行させることができる。

【００２２】

本発明のセキュリティ装置は、デバイス・ベイの蓋部に組み込むことで、コンピュータの余分なスペースを消費することなくオプショナル部品とすることができる。デバイス・ベイの蓋は、セキュリティ装置を組み込んだ蓋とセキュリティ装置を組み込んでいない単なる蓋の二つをオプショナル部品としていずれか一つを選択できるようにし、ユーザまたは販売店でコンピュータに装着できる。

【００２３】

【発明の実施の形態】

［コンピュータ・システムの概要］

図１には、本発明を実施するのに適した典型的なノート型パーソナル・コンピュータ１０のハードウェア構成をサブシステム毎に模式的に示している。ＣＰＵ１１は、ＯＳの制御下で、各種プログラムを実行するようになっている。ＣＰＵ１１は、システム・バス１３を経由して、一般にメモリ／ＰＣＩ制御チップ１５と呼ばれるブリッジ回路（ホスト－ＰＣＩブリッジ）に接続されている。本実施例のメモリ／ＰＣＩ制御チップ１５は、メイン・メモリ１７へのアクセス動作を制御するためのメモリ・コントローラ機能や、システム・バス１３とＰＣＩバス１９間のデータ転送速度の差を吸収するためのデータ・バッファなどを含んだ構

成となっている。

【００２４】

メイン・メモリ１７は、ＣＰＵ１１の実行プログラムの読み込み領域として、あるいは実行プログラムの処理データを書き込む作業領域として利用される、書き込み可能メモリである。ここで言う実行プログラムには、Ｗｉｎｄｏｗｓ９８などのＯＳ、周辺機器類をハードウェア操作するための各種デバイス・ドライバ、特定業務に向けられたアプリケーション・プログラムや、ＦＬＡＳＨ　ＲＯＭ４９に格納されたＢＩＯＳが含まれる。ビデオ・サブシステム２１は、ビデオに関連する機能を実現するためのサブシステムであり、ＣＰＵ１１からの描画命令を実際に処理し、処理した描画情報をビデオ・メモリ（ＶＲＡＭ）に一旦書き込むとともに、ＶＲＡＭから描画情報を読み出して液晶ディスプレイ（図示せず。）に描画データとして出力するビデオ・コントローラを含む。

【００２５】

カードバス・コントローラ２３は、ＰＣＩバス１９のバス・シグナルをＰＣＩカード・スロット２５のインタフェース・コネクタ（カードバス）に直結させるための専用コントローラである。ＰＣＩバス１９とＩ／Ｏバス３９とは、多機能ＰＣＩデバイス２７によって相互接続されている。本実施例の多機能ＰＣＩデバイス２７は、ＰＣＩバス１９とＩ／Ｏバス３９とのブリッジ機能、ＤＭＡコントローラ機能、プログラマブル割り込みコントローラ（ＰＩＣ）機能、及びプログラマブル・インターバル・タイマ（ＰＩＴ）機能、ＩＤＥ（Integrated Drive Electronics）インタフェース機能、ＵＳＢ（Universal Serial Bus）機能、ＳＭＢ（System Management Bus）インターフェース機能を備えており、たとえば、インテル社より提供されているＰＩＩＸ４というデバイスを選択することができる。ＩＤＥインタフェースには、ＩＤＥハードディスク・ドライブ（ＨＤＤ）３１が接続される他、ＩＤＥ　ＣＤ－ＲＯＭドライブ３２が接続される。また、ＩＤＥ　ＣＤ－ＲＯＭ３２ドライブの代わりに、ＤＶＤ（Digital Video Disc又はDigital Versatile Disc）ドライブのような他のタイプのＩＤＥ装置が接続されていても良い。ＨＤＤ３１やＣＤ－ＲＯＭドライブ３２のような外部記憶装置は、例えばシステム１０本体内の「メディア・ベイ」又は「デバイス・ベイ」と呼

ばれる収容場所に格納される。これら標準装備された外部記憶装置は、ＦＤＤやバッテリ・パックのような他の機器類と交換可能かつ排他的に取り付けられる場合もある。

【００２６】

多機能ＰＣＩデバイス２７にはＲＦＩＤタグとしての機能を発揮するＲＦＩＤチップ３３が接続される。ＲＦＩＤチップ３３にはＲＦアンテナ３７が接続される。ＲＦアンテナ３７は、ＨＤＤ３１をコンピュータ１０に収納するためのデバイス・ベイの蓋部に組み込まれている。セキュリティ機能を必要としないユーザは、ＲＦアンテナ３７が組み込まれていないデバイス・ベイの蓋を選択することができる。すなわち、セキュリティ装置の一部としてのＲＦアンテナ３７はオプショナル部品であり、ユーザ自らまたは販売店がアンテナ付き蓋またはアンテナ無し蓋のいずれか一方を装着することができる。ＲＦＩＤチップ３３は、リーダ／ライタが発信したＲＦ励振信号をＲＦアンテナ３７で受信して処理し、コンピュータの不正な持ち出しや不正なアクセスを禁止するセキュリティ機能を備えている。これらの要素はコンピュータ１０のセキュリティ機能の一部を分担しており、後に動作の概要を説明する

【００２７】

Ｉ／Ｏバス３９としては、例えばＩＳＡバスがあり、Ｓｕｐｅｒ　Ｉ／Ｏコントローラ４１、電源コントローラ４５、ＦＬＡＳＨ　ＲＯＭ４９等が接続される。Ｓｕｐｅｒ　Ｉ／Ｏコントローラ４１は、フロッピー・ディスク・ドライブ（ＦＤＤ）の駆動、パラレル・ポートを介したパラレル・データの入出力（ＰＩＯ）、シリアル・ポートを介したシリアル・データの入出力（ＳＩＯ）を制御するための周辺コントローラで、Ｉ／Ｏポート４３が接続される。電源コントローラ４５は主としてシステム内のパワー・マネジメントやサーマル・マネジメントを行うシングル・チップ・マイコンで、日立製作所から提供されるＨ８／３００チップを選定することができる。電源コントローラ４５は、ＭＰＵ、ＲＡＭ，ＲＯＭおよびタイマ等を備え、ＲＯＭにはパワーマ・ネジメントやサーマル・マネジメントを実行するのに必要なプログラムおよび参照テーブルを格納している。電源コントローラ４５には、パワー・サプライ・コントローラ４７が接続されてい

る。パワー・サプライ・コントローラ４７にはバッテリィを充電するための充電器およびコンピュータ１０で使用する５Ｖ、３．３Ｖ等の一定電圧を生成するためのＤＣ／ＤＣコンバータが含まれ、電源コントローラ４５のもとで直接的に電力制御を行う。

【００２８】

ＦＬＡＳＨ　ＲＯＭ４９は、キーボードやフロッピー・ディスク・ドライブ（ＦＤＤ）などの各ハードウェアの入出力操作を制御するためのコード群（ＢＩＯＳ：Basic Input/Output System）や、電源投入時の自己診断テスト・プログラム（ＰＯＳＴ：Power On Self Test）などのファームウェアを恒久的に格納するための書き換え可能な不揮発性メモリである。尚、コンピュータ・システム１０を構成するためには、図１に示した以外にも多くの電気回路等が必要である。但し、これらは当業者には周知であり、また、本発明の要旨を構成するものではないので、本明細書中では省略している。

【００２９】［ＲＦＩＤを利用したセキュリティ機能］

ＲＦＩＤとは一般にＲＦ（Radio frequency）すなわち無線を使って何らかの情報ＩＤ（identification）をＥＥＰＲＯＭに読み書きする機能であるということができる。ＲＦＩＤは単に無線を使った情報交換にとどまらず、一方にリーダ／ライタを配置し他方にＲＦＩＤタグを配置した場合に両者間で情報交換するためにＲＦＩＤタグが電源を必要としないところに最大の特徴がある。リーダ／ライタはＲＦＩＤタグにＲＦ励振信号を送り、ＲＦＩＤタグを励振して電力を発生させてデータを書き込みまたその電力を利用してＲＦＩＤタグがデータをリーダ／ライタに送り返す。このようなＲＦＩＤによるデータの読み書き機能を利用して、電源が停止したコンピュータとリーダ・ライタとの間で多くの情報を交換することができコンピュータの在庫管理等に利用できる。

【００３０】

ＲＦＩＤの他の利用形態としてコンピュータのセキュリティ機能に関するものがある。図２は、ＲＦＩＤタグとしてのＲＦＩＤチップ３３の内部構成を概略的に記載したものである。このようなＲＦＩＤチップとしては、ＡＴＭＥＬ社から提供されるＡＴ２４ＲＦ０８という型式のＥＥＰＲＯＭ（Asset Identification

EEPROM）がある。ＲＦＩＤチップ３３に含まれるＥＥＰＲＯＭ５５は、記憶領域が８Ｋビットの一般エリア５７と２５６ビットの特殊エリア５９に分割されている。一般エリア５７には、ＲＦアンテナ３７で受信したＲＦ励振信号のデータがアナログ・インタフェース５３を経由して書き込まれ、また書き込まれているデータはインターフェース５３およびＲＦアンテナ３７を経由して発信される。またＥＥＰＲＯＭ５５とコンピュータ１０はシリアル・インタフェース６１およびＳＭＢ３５を通じて通信し、コンピュータから一般エリア２７および特殊エリア５９への書き込みおよび読み出しができる。さらに、一般エリア５７には本発明の実施例として二つの記憶領域が設けられている。一つは、ＲＦアンテナの装着状況の履歴を示すＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットで、コンピュータ１０へＲＦアンテナが装着されたことが検出されると「１」にセットされる。もう一つは、Ａｎｔｅｎｎａ　Ｅｒｒｏｒビットで、一旦装着されたＲＦアンテナ３７が脱着されたことが検出されると「１」にセットされる。Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットおよびアンテナ　Ｅｒｒｏｒビットは適切なパスワードを保有するユーザがＳＭＢ３５およびシリアル・インターフェース６１を経由してコンピュータ・システムからＥＥＰＲＯＭ５５にアクセスしない限りリセットできない。

【００３１】

特殊エリア５９には、ＲＦアンテナ３７のコンピュータ１０に対する着脱状態を検出するためのＤＥ／ＤＣビット領域、ＲＦアンテナ３７が監視区域のゲート近くに設置されたリーダ／ライタからＲＦ励振信号を受信したときにセットするＴａｍｐｅｒビット領域、一般エリア５７へのリード、ライトをロックするＡｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビット領域、およびコンピュータの電源がオフになるまでＡｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビットの変更をロックするＳｔｉｃｋｙビット等が含まれる。Ａｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビットは２ビットで構成され、「００または０１」のときは一般エリアへの一切のアクセスが禁止され、「１０」のときは読み出しだけが許可され、「１１」のときは書き込みおよび読み出しが許可される。

【００３２】

ＤＥ／ＤＣビット領域は、ＤＥビット（Detect Enable bit）とＤＣビット（Detect Coil bit）からなる。ＲＦＩＤチップ３３は、シリアル・インターフェース６１を通じてＤＥビットが「１」にセットされるとＲＦアンテナ３７の着脱状態をチェックし、ＲＦアンテナ３７が装着されているときは「１」を、脱着されているときは「０」をＤＣビットに書き込むようになっている。コンピュータの電源が入っている場合は電源部５１がアナログ・インターフェース５３を駆動するが、電源がない場合はＲＦアンテナ３７を通じて受信したＲＦ励振信号がアナログ・インタフェース５３を駆動し、電源がない状態でもリーダ／ライタと通信できる。

【００３３】［本発明の実施例を適用するセキュリティ機能の概要］

次に本発明の実施例を適用するコンピュータのセキュリティ機能の概要を説明する。電源がオフになっているコンピュータが監視区域のゲートに近づくと、リーダ／ライタが発信するＲＦ励振信号がＲＦアンテナ３７に送られ、ＥＥＰＲＯＭ５５の特殊エリア５９にＴａｍｐｅｒビットがセットされる。つぎにコンピュータの電源を投入すると、ＦＬＡＳＨ　ＲＯＭ４９に格納されているＢＩＯＳがメイン・メモリ１７に書き込まれ、ＣＰＵ１１はＰＯＳＴおよびシステムの初期化を実行する。ＰＯＳＴがＴａｍｐｅｒビットを検出するとパスワードの入力をユーザに要求すると共にその時点でＰＯＳＴの実行を停止し、パスワードの入力がない限りコンピュータへアクセスすることはできなくなる。

【００３４】

前述のようにＲＦアンテナ３７はユーザまたは販売店が装着できるようにしているため、不正にコンピュータを外に持ち出そうとする者がＲＦアンテナ３７を外してからゲートを通過し、Ｔａｍｐｅｒビットがセットされるのを回避しようとする可能性がある。本発明の実施例では、ＲＦアンテナ３７はオプションとして取り付けるが、その他のハードウエアはＲＦアンテナ３７を装着する場合と脱着する場合とで共通である。また、ＲＦアンテナ３７を装着する場合とＲＦアンテナを脱着する場合のいずれにおいても同一のソフトウエア（ＢＩＯＳ）を採用できる。以下において、ＲＦアンテナ３７が不正に脱着された場合にコンピュータへのアクセスを禁止するための手順の実施例を説明する。

【００３５】［本発明の手順を示す第一の実施例］

図３は本発明の手順を示す第一の実施例としてのフローチャートである。コンピュータ１０にＲＦアンテナが実際に装着されてセキュリティ機能が有効になるか否かは、この時点でシステムにとって不明である。コンピュータ１０のＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットおよびａｎｔｅｎｎａ　Ｅｒｒｏｒビットは、工場から出荷する時点では共に「０」にセットされている。ブロック１０１でコンピュータ１０の電源をオンにすると、ＢＩＯＳがＦＬＡＳＨ　ＲＯＭ４９からメイン・メモリ１７に読み出され、ＣＰＵ１１がＰＯＳＴプログラムを読みとって以下の手順を実行する。ＲＦＩＤチップ３３は、電源投入時点では常にＡｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビットが「１１」にＳｔｉｃｋｙビットが「１」にセットされ、一般エリア５７へのＢＩＯＳによるアクセスが許可される。ブロック１０３でＰＯＳＴは現実にＲＦアンテナ３７がコンピュータに装着されているか否かを確認するために特殊エリア５９のＤＥビットを「１」にセットする。これに応じてＲＦＩＤチップ３３はＲＦアンテナ３７の装着状態をチェックし、装着されていればＤＣビットに「１」を脱着されていれば「０」を書き込む。

【００３６】

ＰＯＳＴはＤＥビットを「１」にセットしてから約２００マイクロ秒経過した後ＤＣビットを読みとり、さらにＤＥビットを「０」にセットする。ＤＣビットが「１」にセットされて現在ＲＦアンテナ３７が装着されていることが確認されたならばブロック１０５に移行して一般エリア５７のＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットを「１」にセットする。この時点で、コンピュータ１０がセキュリティ機能を具備するコンピュータであることがシステムによって認識されたことになり、以後Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットは、パスワードを有するユーザが書き換えない限り電源がオフになってもこの情報を維持し続ける。ＤＣビットが「０」でＲＦアンテナが脱着されていることが確認されたならば、ブロック１０７に移行して一般エリア５７のＡｎｔｅｎｎａ　Ｅｒｒｏｒビットを確認する。Ａｎｔｅｎｎａ　Ｅｒｒｏｒビットをこの時点で確認することは、後にブロック１０９で詳細に説明するが、前回のＰＯＳＴを実行する以前に一旦装着されたＲＦアンテナが脱着されたことがあったか否かを確認することに相当する。

【００３７】

ブロック１０７でＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「１」のときは、前回のＰＯＳＴを実行する以前にＲＦアンテナ３７が一旦装着され、さらに前回のＰＯＳＴを実行する段階でＲＦアンテナ３７が脱着されていた場合であり、ＲＦアンテナの不正な脱着があったものとしてこれを処理するブロック１１９に移行する。以後Ａｎｔｅｎｎａ　Ｅｒｒｏｒビットは、パスワードを有するユーザが書き換えない限り電源がオフになってもこの情報を維持し続ける。ブロック１０７でＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「０」のときは、すくなくとも前回のＰＯＳＴの実行時点まではＲＦアンテナの不正な脱着がなかったものと判断し、ブロック１１１に移行する。

【００３８】

ブロック１１１では、Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットを確認する。すなわち、今回のＰＯＳＴを実行する時点までにＲＦアンテナ３７がコンピュータ１０に装着されたことがあるか否かを確認する。Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットへのデータは、ブロック１０５により今回のＰＯＳＴ実行時に、または前回以前のＰＯＳＴ時に書き込まれる。ブロック１１１でＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットが「０」のときは、現在までＲＦアンテナが装着されたことがない場合であってコンピュータ１０はセキュリティ機能を有しないコンピュータであることを意味しており、ブロック１１５に移行する。ブロック１１１でＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットが「１」のときは、今回のＰＯＳＴを実行する時点までにＲＦアンテナが装着されたことがあり、かつ前回のＰＯＳＴを実行する時点までの間に一旦装着されたＲＦアンテナが脱着されたことがＰＯＳＴで検出されていない場合（Ａｎｔｅｎｎａ　Ｅｒｒｏｒビット＝０）であり、ブロック１１３に移行する。

【００３９】

ブロック１１３ではＤＣビットを再度確認し、今回のＰＯＳＴ実行時点でＲＦアンテナ３７が装着されているか脱着されているかを判断する。ＤＣビットが「１」すなわち現実にＲＦアンテナ３７がコンピュータ１０に装着されていれば、セキュリティ装置の脱着はなかったものとしてブロック１１５に移行する。ＤＣ

ビットが「０」のときは、今回のＰＯＳＴを実行する以前にＲＦアンテナが装着されていたが（ブロック１１１）今回のＰＯＳＴを実行する段階では脱着されており（ブロック１１３）、さらに前回のＰＯＳＴを実行する以前に一旦装着されたＲＦアンテナが前回以前のＰＯＳＴを実行する段階で脱着されたことが検出されていない（ブロック１０７）場合であり、ブロック１０９に移行して処理される。言い換えると、これは前回のＰＯＳＴを実行してから今回のＰＯＳＴを実行するまでの間にＲＦアンテナが脱着された場合を今回のＰＯＳＴで処理する手順である。前回のＰＯＳＴを実行する時点においてそれまでに一旦装着されたＲＦアンテナ３７が脱着されていると、前回のＰＯＳＴを実行する時点でＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「１」にセットされ、今回のＰＯＳＴを実行するとブロック１０７からブロック１１９に移行して処理されるからである。

【００４０】

ブロック１１５は、ブロック１１１から移行する手順で示されるセキュリティ機能を有しないコンピュータと、ブロック１１３から移行する手順で示されるセキュリティ機能を有しかつＲＦアンテナ３７が一旦装着された後に脱着されたことがないコンピュータとを処理する。この場合は、セキュリティ装置の脱着はないので、Ａｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビットを「１０」にセットし、以後一般エリアのＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットおよびアンテナ　Ｅｒｒｏｒビットへの書き込みを禁止する。さらにＳｔｉｃｋｙビットを「０」にセットして、コンピュータの電源が切られるまでＡｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビットの変更ができないようにする。これは、ＯＳ経由でＡｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビットが「１１」に変更され、Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットまたはアンテナ　Ｅｒｒｏｒビットの内容が書き換えられるのを防止するためである。この結果Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットおよびアンテナ　Ｅｒｒｏｒビットの書き換えは、電源がオンになったブロック１０１からブロック１１５までの間だけ可能になり、実際はこの間にＰＯＳＴだけがビットの書き換えをすることになる。続いてブロック１１７に移行し、ＢＩＯＳはブートストラップを実行し、ＯＳおよびアプリケーション・プログラムをメイン・メモリに読み出しコンピュータの構成を行う。

【００４１】

ブロック１０９ではＡｎｔｅｎｎａ　Ｅｒｒｏｒビットを「１」に書き換える。Ａｎｔｅｎｎａ　ＥｒｒｏｒビットはＰＯＳＴを実行する毎にブロック１０７ないしブロック１１３が判断され、その結果に応じて「１」に書き換えられる。ブロック１０９は、前回のＰＯＳＴを終了した時点ではＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「１」に書き換えられていなかったが（ブロック１０７）、今回のＰＯＳＴを実行した時点で過去においてＲＦアンテナ３７が装着されたことがある（ブロック１１１）にも係わらず現在それが脱着されている（ブロック１１３）場合を処理する。

【００４２】

続いてブロック１０９からブロック１１９に移行する。さらにブロック１０７で判断したＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「１」である場合もブロック１１９に移行する。ブロック１１９では今回のＰＯＳＴを実行する間にブロック１０９によりＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「１」にセットされた場合および前回のＰＯＳＴを終了するまでの間にＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「１」であったことに応答してコンピュータ１０のディスプレイにＰＯＳＴエラーの表示をする。

【００４３】

次にブロック１２１でディスプレイにユーザにパスワードを要求するメッセージを表示し、ＢＩＯＳがブロック１２３で正しいパスワードの入力を認識すると、ブロック１２７でＡｎｔｅｎｎａ　ＨｉｓｔｏｒｙビットおよびＡｎｔｅｎｎａ　Ｅｒｒｏｒビットを「０」に書き換える。続いてブロック１２９でＰＯＳＴを再スタートする。再スタートしたＰＯＳＴでは、ＰＯＳＴエラーの表示がでることはなくブロック１０１からブロック１１７までの手順をクリアしてブートストラップが実行される。

【００４４】

ＢＩＯＳがブロック１２３で正しいパスワードを認識しないとその時点でＰＯＳＴは停止し、以後コンピュータへのアクセスはできなくなる。それ以降正しいパスワードを入力できる場合は、再度ブロック１０１の電源オンからスタートし

て、ブロック１２１で正しいパスワードを入力してからブロック１２９を経由して再度ブートストラップを実行する。

【００４５】［本発明の手順を示す第二の実施例］

図３のフローチャートで説明した手順では、電源がオンの状態でＲＦアンテナが不正に外されてコンピュータが外部に持ち出されても、一旦電源をオフにしてＰＯＳＴを実行する段階にならないとコンピュータへのアクセスを禁止することはできない。電源オンの状態でＲＦアンテナが外されてしまうことに対処するために、本発明の手順を示す第二の実施例としてのフローチャートを図４に示す。電源が投入され、図３で説明した手順でＰＯＳＴが実行されてブースストラップが開始されると、デバイス・ドライバによってブロック１５１から始まる第二の実施例の手順が開始される。ブロック１５３ではＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットが確認される。今回のＰＯＳＴを実行する時にＲＦアンテナが装着されていれば図３のブロック１０５でＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットは「１」にセットされている。ブロック１５３では、Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットを確認し、ビットが「０」でＲＦアンテナが装着されていなければブロック１５７へ移行し本手順は終了する。

【００４６】

ブロック１５３で確認したビットが「１」で今回のＰＯＳＴを実行した時点でＲＦアンテナが装着されていれば、ブロック１５５に移行する。ブロック１５５でポーリングにより定期的にＤＣビットの状態を確認する。このポーリングは実際には他のプログラムの実行を妨げないように、タイマー・インターラプトなどによって行われることが好ましい。ＲＦアンテナ３７が脱着されない限りＣＰＵはＲＦアンテナの装着状態を定期的に監視する。ＲＦアンテナ３７が脱着されるとブロック１５９に移行しコンピュータの電源が強制的にオフにされるので、ユーザが再度電源をオンにすると図３に示したＰＯＳＴが再スタートさせられる。図３の手順ではブロック１０３、１０７、１１１、１１３、１０９、１１９、１２１のルートに従って処理され、パスワードが要求される。すなわちコンピュータの電源オンの状態において、一旦装着されたＲＦアンテナ３７が脱着されると、ＣＰＵ１１のポーリングのタイミングでコンピュータの電源がオフにされるの

で、次回の電源をオンにしたときＰＯＳＴが実行され、パスワードを入力できないユーザはそれ以上コンピュータにアクセスできないことになる。

【００４７】

以上本発明の手順をＢＩＯＳのＰＯＳＴで実行する場合を例にして説明してきたが、本発明を実行するプログラムはＰＯＳＴに限定されるものではなく、他のＢＩＯＳ、デバイス・ドライバ、ＯＳ、またはアプリケーション・ソフトといわれる各種ソフトウエアを利用して実行することができる。ＰＯＳＴ以外のソフトウエアを利用する場合には、図３に示した手順を開始するタイミングとして、ユーザが特定のデータにアクセスした場合や、サスペンドまたはハイバーネーションといわれるような各種省エネ・モードに移行した場合等を採用することができる。

【００４８】

図５に本発明を実行するコンピュータ１０の外形の一例を示す。コンピュータ１０は図１で説明した構成要素を収納する本体２０１、液晶ディスプレイ２０３，本体上部に配置したキーボード２０７、ＣＤ－ＲＯＭドライブ３２、およびＨＤＤ３１を収納するデバイス・ベイの蓋２０９を含む。コンピュータ１０はデバイス・ベイの蓋２０９を除いて、本実施例との関連で特別な外形的特徴を備えるものではない。

【００４９】

図６に本発明で使用するＲＦアンテナ３７の装着方法の実施例を示す。ＲＦアンテナ３７はデバイス・ベイの蓋２０９に収納される。デバイス・ベイにＨＤＤ３１が着脱可能な状態で装着した後に蓋２０９を本体２０１に対してはめ込み構造で取り付ける。ＲＦアンテナ３７を使用しない場合、すなわちセキュリティ機能を必要としないコンピュータでは、ＲＦアンテナ３７を取り付けないで蓋２０９だけを本体２０１に装着できる。また、蓋２０９とは異なりＲＦアンテナ３７を収納できない構造の蓋を用意してもよい。このようなＲＦアンテナ３７の取り付け構造を蓋２０９に採用することにより、ユーザまたは販売店でＲＦアンテナ３７の取り付けが可能になり、ユーザはセキュリティ機能の必要性に応じてＲＦアンテナ３７付きの蓋２０９またはＲＦアンテナ３７なしの蓋２０９のいずれか

を選択できる。蓋２０９の内側には、アンテナ３７用コイルが収納され、そのリード部２１１は蓋２０９の端子部にはめ込まれると共に、ＲＦＩＤチップ３３に電気的に接続される。

【００５０】

このような方法でＲＦアンテナ３７を取り付ける場所としては、ＨＤＤ用のデバイス・ベイの蓋部にとどまらずＣＤ－ＲＯＭドライブ、ＤＶＤドライブ、ＦＤＤ、バッテリィ等の外部装置のデバイス・ベイの蓋や、これらを択一的に収納できるマルチ・ベイの蓋を利用できる。ＲＦアンテナ３７の本体２０１に対する取り付け構造は、コンピュータの使用場所において不正行為者が短時間に脱着できるものではなく、かつ販売店またはユーザがある程度の時間を費やして着脱できる程度に強固なものであることが好ましい。たとえば、はめ込み構造に加えてスクリューで締め付ける構造や、そのスクリューに特殊な工具を要するものを採用することができる。

【００５１】

本発明の実施例はＲＦＩＤを利用したセキュリティ装置の脱着が行われたときにコンピュータへのアクセスを禁止する例で説明したが、本発明の適用範囲はＲＦＩＤに限定されるものではなく、たとえば指紋によりコンピュータへのアクセス資格を確認するような他の種類のセキュリティ装置にも適用できる。

【００５２】

【発明の効果】

本発明により、セキュリティ装置が不正に脱着されたときにアクセスができなくなるコンピュータを提供することができた。さらに本発明によりセキュリティ機能の有無だけが相違するコンピュータにおいて、セキュリティ装置以外はハードウエアおよびソフトウエアが共通なコンピュータを提供することができた。また本発明により、装着および脱着が可能で余分なスペースを必要としないセキュリティ装置の取り付け構造を備えたコンピュータを提供することができた。

【図面の簡単な説明】

【符号の説明】

【図１】本発明を実施するコンピュータの概略ブロック図の一例である。

【図２】本発明の実施例で使用するＲＦＩＤチップの概略ブロック図である。

【図３】本発明の手順を示す第一の実施例のフローチャートである。

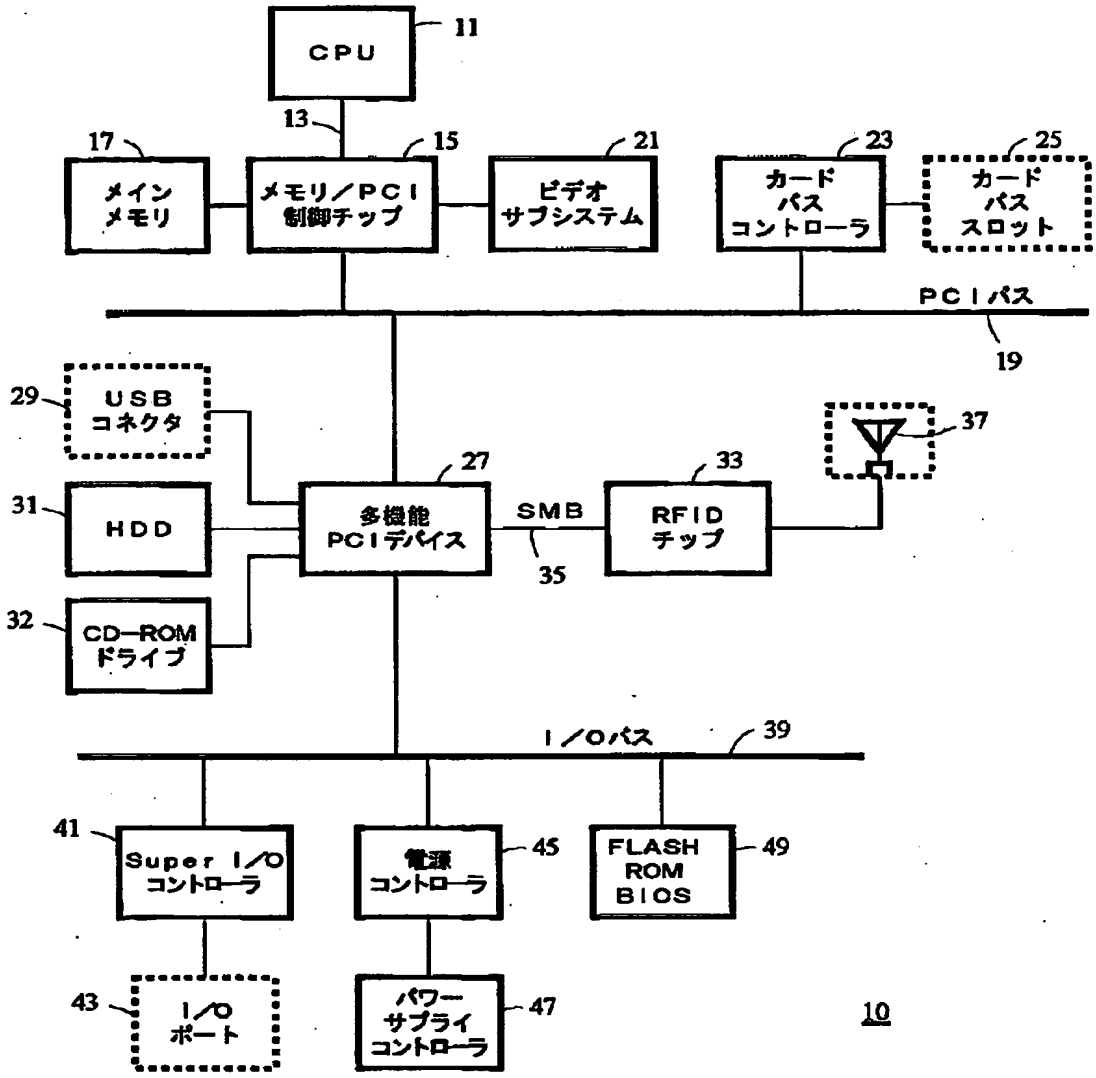
【図４】本発明の手順を示す第二の実施例のフローチャートである。

【図５】本発明を実施するコンピュータの外形図の一例である。

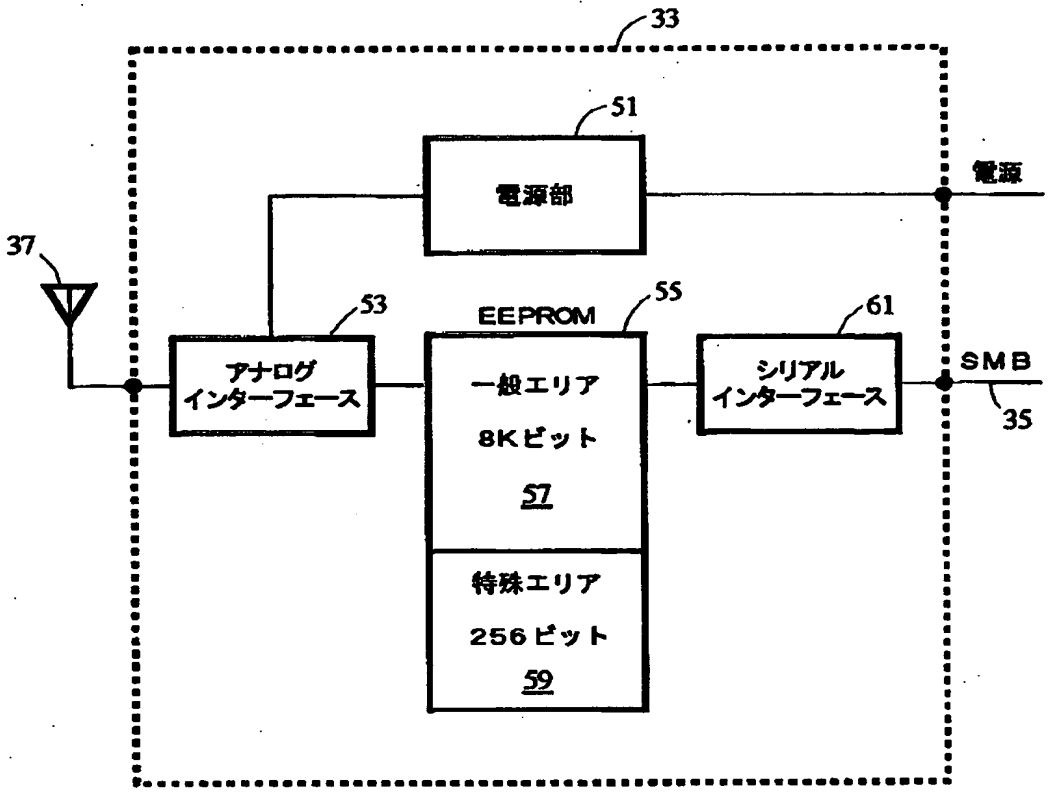
【図６】本発明の実施例で使用するＲＦアンテナの取り付け方法の一例を示す図である。

【書類名】　図面

【図１】

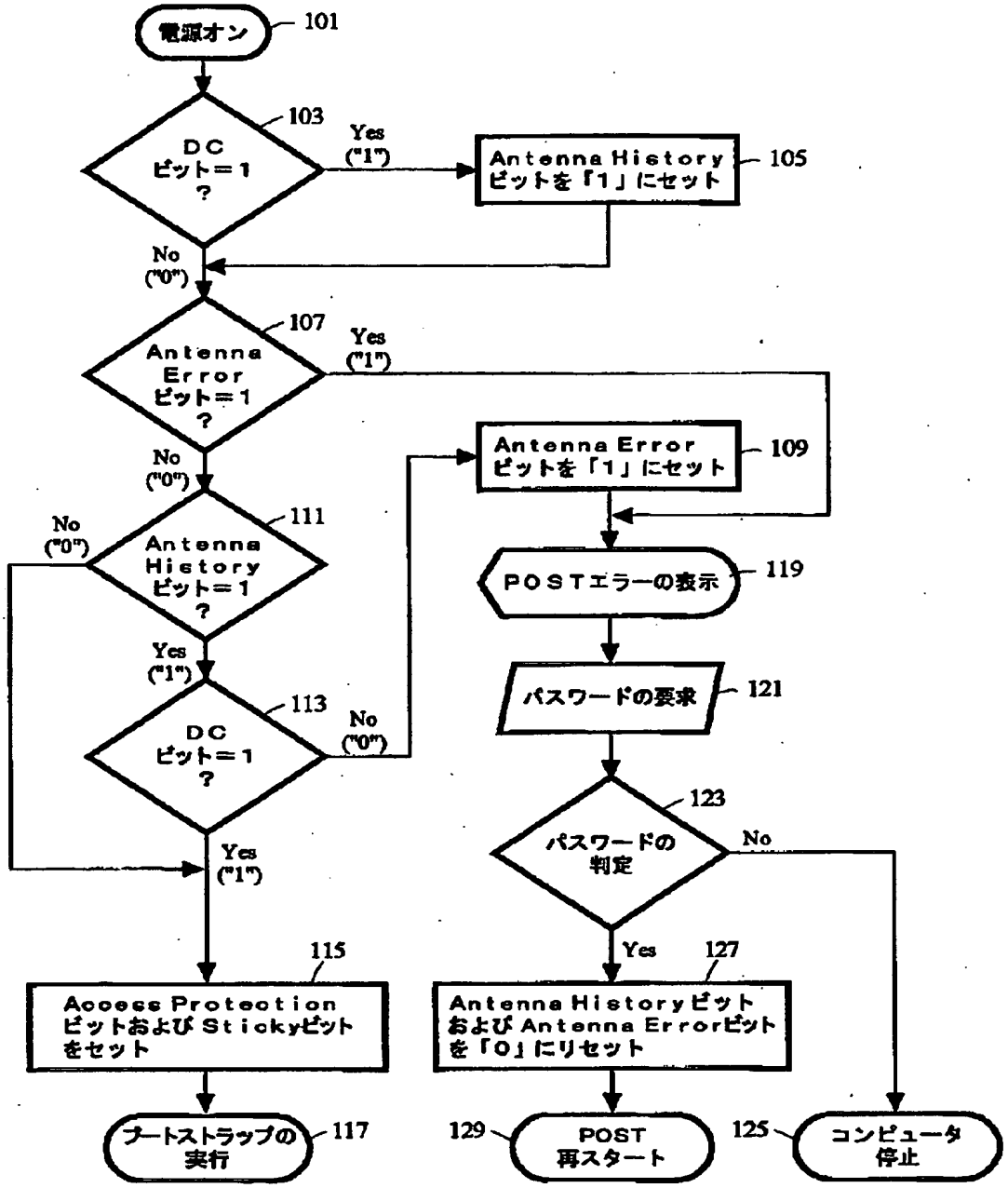

CPU
11
13
17
メイン
メモリ
15
メモリ／PCI
制御チップ
21
ビデオ
サブシステム
23
カード
バス
コントローラ
25
カード
バス
スロット
PCIバス
19
29
USB
コネクタ
37
27
33
31
HDD
多機能
PCIデバイス
SMB
RFID
チップ
35
32
CD-ROM
ドライブ
I／Oバス
39
41
Super I／O
コントローラ
電源
コントローラ
45
FLASH
ROM
BIOS
49
43
I／O
ポート
パワー
サプライ
コントローラ
47
10

【図２】

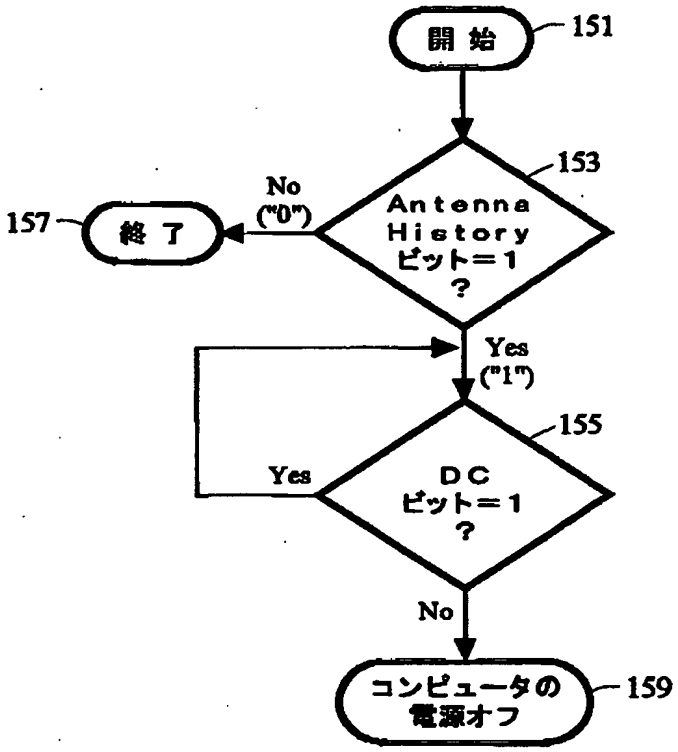


出証特平１１－３０２９３９９

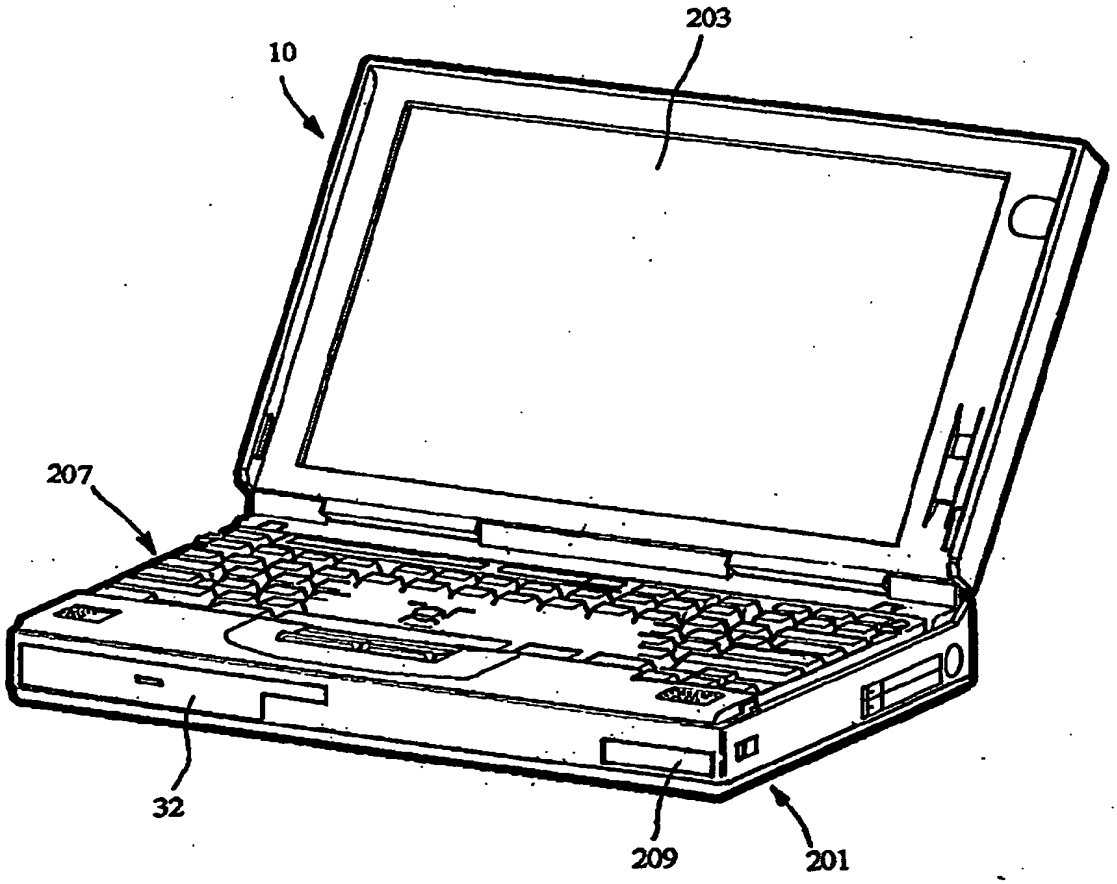
【図３】


電源オン
101
DC ビット＝1 ？
103
Yes ("1")
Antenna History ビットを「1」にセット
105
No ("0")
Antenna Error ビット＝1 ？
107
Yes ("1")
No ("0")
Antenna Error ビットを「1」にセット
109
No ("0")
Antenna History ビット＝1 ？
111
Yes ("1")
DC ビット＝1 ？
113
No ("0")
Yes ("1")
POSTエラーの表示
119
パスワードの要求
121
パスワードの判定
123
No
Yes
127
Access Protection ビットおよびStickyビットをセット
115
Antenna History ビットおよびAntenna Errorビットを「0」にリセット
ブートストラップの実行
117
129
POST 再スタート
125
コンピュータ停止

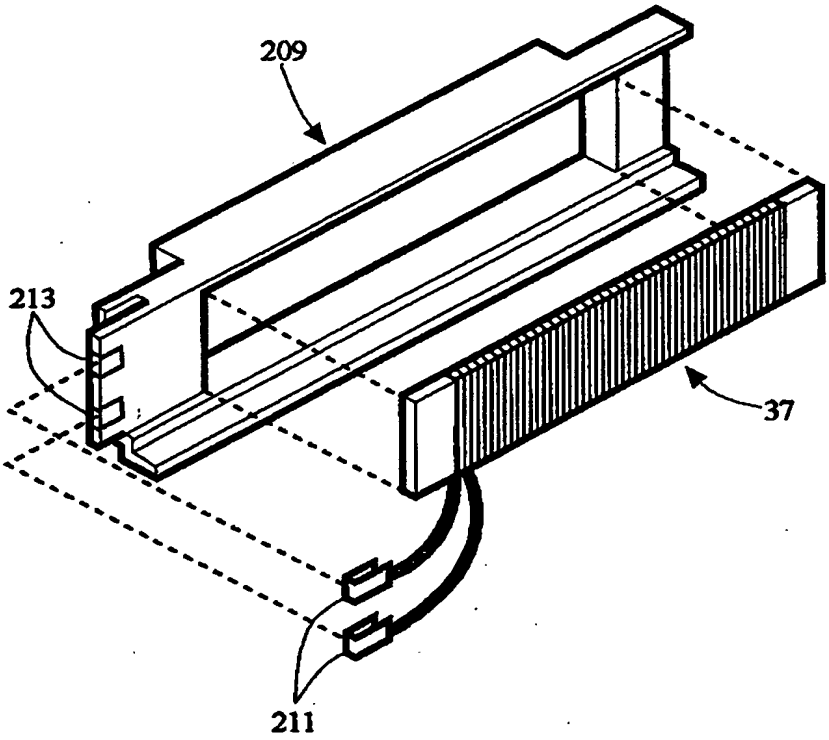
【図４】


開 始
151
153
Antenna History ビット＝1 ？
No ("0")
157
終 了
Yes ("1")
155
DC ビット＝1 ？
Yes
No
コンピュータの電源オフ
159

【図５】



【図６】



【書類名】　要約書

【要約】

【課題】セキュリティ機能付きコンピュータのセキュリティ装置が不正に取り外された場合にコンピュータへのアクセスを禁止する技術を提供する。

【解決手段】セキュリティ装置はコンピュータのセキュリティ機能の一部を担うハードウエアであり、不正に脱着された場合に以下の手順でアクセスを禁止する。コンピュータにセキュリティ装置が装着されたこと示すデータを不揮発性メモリに記憶し保持する。そのあとに電源オン等の何らかのイベントをきっかけとしてコンピュータへのアクセスを禁止する手順を開始する。続いてメモリのデータに基づいてセキュリティ装置が装着されたことがあることを検出する。さらにコンピュータから現在セキュリティ装置が脱着されていることを検出する。セキュリティ装置が装着されたことがあるにも係わらず現在脱着されているならば、コンピュータへのアクセスを禁止する。

【選択図】図３

認定・付加情報

特許出願の番号	平成１１年　特許願　第０１３２１５号
受付番号	５９９０００４９４１０
書類名	特許願
担当官	第二担当上席　　００９１
作成日	平成１１年　１月２５日

＜認定情報・付加情報＞

【提出日】　平成11年 1月21日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔３９０００９５３１〕

１．変更年月日　　１９９０年１０月２４日
［変更理由］　新規登録
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレイション